

## Secure Information Sharing Architecture, Part 3: Monitoring Security-Policy Compliance and Stopping Violations

*By Chris Shenefiel, Federal Government Industry Solutions Manager, Cisco and Susan Shareshian, Solution Development Manager, Federal Center of Excellence, Cisco*

*In previous issues of this newsletter, we introduced the Cisco Secure Information Sharing Architecture (SISA) and discussed two of its four layers: [access control services](#) and [data protection services](#). This article discusses another of the four layers: watchdog services.*

In the federal government, communities of trust must share information and collaborate, whether to help keep the peace, respond to humanitarian needs, manage intelligence data, or promote commerce. The Secure Information Sharing Architecture (SISA), which combines products and expertise from Cisco, EMC, Microsoft, and other companies, enables agencies to confidently share sensitive materials across organizational boundaries. Each agency in the community of trust can determine how, when, where, and with whom it will share its information, according to the requirements of the mission.

SISA comprises four architectural service layers: access protection, content protection, data protection, and watchdog services.

### **Watchdog Services: Guarding the Gate**

Watchdog services monitor network resources on the SISA to ensure that they are being used according to the organization's security policy, and block events that violate policy. Watchdog services also create a central log of all network activity so that all members in a community of trust know where their information goes, who is using it, and how.

One of the main technologies behind watchdog services is the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS). Suppose an individual is attempting to copy a file onto a USB drive, and that the agency's policy forbids this action. Cisco Security Agent, installed on the desktop, enforces the policy by preventing the action, and then Cisco Security MARS centrally records the event for later forensic activities.

Cisco Security MARS detects and blocks more complex threats, as well. For example, it can analyze and correlate thousands of events happening at the same time in different parts of the network, recognize them as part of a unified attack, and automatically notify the appropriate response team. Agencies can also configure Cisco Security MARS to automatically issue commands to mitigate the impact of the attack.

### **Monitoring Compliance with STIG, IPv6, and FISMA**

Cisco Security MARS plays an essential role in the SISA by enforcing the agency's security policies. But how can an agency confirm that its security policies are compliant with federal regulations, such as Security Technical Implementation Guidelines (STIG), IPv6 requirements, and the Federal Information Security Management Act (FISMA)? The need to monitor compliance

is constant because agencies can become out of compliance through such everyday events as changing a router configuration or adding or removing a network device.

Compliance monitoring has traditionally been manual and time consuming. For STIG compliance, for example, network managers typically perform ad hoc network scans and then manually validate the results against a large text-based rule set. This painstaking process takes so long that one report might not be complete before the next report is due. As a result, some agencies resort to scanning just one part of the network rather than the entire network, potentially overlooking policy violations that could compromise the security of sensitive government information. The situation is no better for IPv6 compliance reporting, to which one federal agency has dedicated three full-time resources.

### On-Demand Compliance Reporting

The CiscoWorks Network Compliance Manager complements watchdog services by monitoring the network for compliance with STIG, IPv6, and FISMA. Rules are embedded in the appliance and updated automatically, through a subscription service. When policy violations are detected, the solution immediately notifies the network management team by cell phone, e-mail, or text message so that they can correct the problem before harm is done. Agencies can also generate STIG, IPv6, and FISMA compliance reports on demand, sparing themselves the weeks or months of effort currently required.

To read more about SISA, visit: [www.cisco.com/go/sisa](http://www.cisco.com/go/sisa).

To find out about the CiscoWorks Network Compliance Manager, visit the Cisco Center for Excellence at [www.cisco.com/web/strategy/government/coe\\_index.html](http://www.cisco.com/web/strategy/government/coe_index.html).



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)